ITRMC Information Technology Policies

ENTERPRISE STANDARDS – S3000 NETWORK AND TELECOMMUNCATIONS

Category: S3240 – **SECURITY – PUBLIC-FACING WEB SERVERS**

CONTENTS:

I. DEFINITION

A public-facing web server is any server which hosts a web site or application which is accessible from the internet.

II. RATIONALE

Idaho State government is responsible for protecting sensitive and business-critical information on the government network. Each agency and the state government as a whole must ensure safe practices are in place to reduce the risk that information will be lost, stolen or changed.

III. APPROVED STANDARD

A. Protection of Sensitive Data
Sensitive data is prohibited from being stored persistently on a public-facing web server. Sensitive data includes but is not limited to the following:

- Protected Health Information
- Personnel-Employee Records
- Social Security Numbers
- Personally Identifiable Data
- Driver’s License Numbers
- Financial Records
- Application and database IDs (logon credentials)
- Vulnerability Assessment/Audit Technical Detail

- Detailed Technical Information (including passwords)
- Facility Security Information
- Education-Student Records
- Investigative and court information

B. Overview of required actions:

1. All future public-facing web servers will be on the state's enterprise DMZ.
2. Agencies with current public-facing web servers on the state's internal network, will move those servers to the state's enterprise DMZ by December 31, 2012.
3. Public-facing web servers and associated web applications will be certified to ensure they meet minimum security standards.
4. Database servers which interface with public-facing web servers must meet minimum required security standards as detailed in section IV of this standard.
5. Public-facing web servers will have logging enabled and will be configured to send pertinent log data to the OCIO Security Information and Event Management (SIEM) device.

IV. TECHNICAL AND SECURITY IMPLEMENTATION CONSIDERATION

A. Public-Facing Web Servers on Enterprise DMZ

In following Best Practices for Information Technology, all future public-facing web servers will be required to be placed on the state's enterprise DMZ in coordination with the OCIO. Current public-facing web servers will need to make the transition within two years. By ensuring all public-facing web servers are on the DMZ, the State of Idaho will significantly reduce the risk of network attacks affecting sensitive information and resources.

B. Web Certification Process

1. All future public-facing web servers must be certified using the following certification process (current public-facing web servers must make this transition within two years):
   a) The Center for Internet Security (CIS) Benchmark should be referenced for configuration settings for the web/IIS server running on that operating system, provided on the OCIO security website (CIS IIS document) must be completed by the system administrator and the web server administrator and signed by both to indicate compliance.
   b) The checklists will then be submitted to the OCIO Security Team and vulnerability scans of the server will be performed to confirm compliance with the security settings.
   c) Public-facing web servers will be re-certified on a biannual basis.

2. All web applications that are publicly accessible must be certified using the following certification process:
   a) The Microsoft Application Security: Threats and Countermeasures document should be referenced for configuration settings for web applications (MS Web

App Document). System specific checklists included in the document provide solid industry standard security practices for web applications.

b) The appropriate checklist must be completed by the web application technician who is responsible for the application.

c) The signed checklist will then be submitted to the OCIO Security Team and a web application vulnerability scan will be performed to confirm compliance.

d) Externally developed web applications that reside on state web servers must abide by the web application certification process and will be subject to the same web application vulnerability scans to confirm compliance.

3. Web application programmers/developers must keep up to date with emerging security threats that affect web applications by completing annual security awareness training on secure web application development, provided by the Office of the CIO, or equivalent training.

C. Web Application Databases

The following requirements apply to database servers that interface with public-facing web applications:

1. Desktop Database Management Systems such as Microsoft Access must not be used for enterprise applications and must not be used to store sensitive information.
2. A Database Management System must be housed on a dedicated server and must not reside on a server that has multiple functions such as one that also operates as a file server, web server or domain controller.
3. The Center for Internet Security (CIS) Benchmarks should be referenced for configuration settings for SQL Server and Oracle should be used as a check on running systems and as a standard when configuring security settings for new systems (CIS SQL and Oracle Documents).
4. Web applications that connect to backend database servers must do so with encrypted credentials so that the password for the application account is never visible in any HTTP application code.
5. Servers on the Enterprise DMZ will not also be connected to the state internal network; this applies to hardware containing multiple virtual server instances as well.

D. Security Logging

Public-facing web and database servers will have logging enabled and will be configured to send pertinent log data to the OCIO SIEM device so that events can be correlated and anomalies detected.

V. ENFORCEMENT AND EXCEPTIONS

1. Violation of this standard will result in the removal of a website from the state network.
2. Exceptions to this can only be approved by the OCIO and will require additional security measures to ensure protection of the state network. These measures will include two or more of the following:

a) A Host Intrusion Protection System (HIPS) which will prevent most attacks and will provide logs of data to the OCIO. The HIPS must meet all other ITRMC standards or be specifically approved by the OCIO.
b) A file integrity monitoring solution (e.g., Tripwire) which will report any file and data changes on server systems to the OCIO.
c) Daily manual auditing of event and security logs of the web server and any server with which it interfaces.

3. Requests for exceptions to the requirements of this standard should be made to the OCIO. Please complete and submit the ITRMC Exception form that is located at http://www2.state.id.us/itrmc/plan&policies/Exemption_Request_Form.xls (hard copy or email) to the OCIO.

VI. REVIEW CYCLE

Six (6) Months

VII. TIME LINE

Effective Date: June 24, 2009

VIII. REVISION HISTORY